

NEW YORK
LONDON
SINGAPORE
PHILADELPHIA
CHICAGO
WASHINGTON, DC
SAN FRANCISCO
SILICON VALLEY
SAN DIEGO
LOS ANGELES
TAIWAN
BOSTON
HOUSTON
AUSTIN
HANOI
HO CHI MINH CITY

DuaneMorris®

FIRM and AFFILIATE OFFICES

WILLIAM K. KEANE
DIRECT DIAL: +1 202 776 5243
PERSONAL FAX: +1 202 478 2160
E-MAIL: KKeane@duanemorris.com

www.duanemorris.com

SHANGHAI
ATLANTA
BALTIMORE
WILMINGTON
MIAMI
BOCA RATON
PITTSBURGH
NEWARK
LAS VEGAS
CHERRY HILL
LAKE TAHOE
MYANMAR
OMAN
*A GCC REPRESENTATIVE OFFICE
OF DUANE MORRIS*
ALLIANCES IN MEXICO
AND SRI LANKA

August 17, 2021

Marlene H. Dortch, Secretary
Federal Communications Commission
45 L Street NW
Washington, DC 20554

**Re: WC Docket 18-89 and
ET Docket 21-232 and EA Docket 21-233
Ex Parte Presentation**

Dear Ms. Dortch:

On behalf of Hytera Communications Corporation Limited (HCC) and its subsidiary, PowerTrunk, Inc. (PowerTrunk), I am writing to inform you that Patrick McPherson and I, along with Marjorie K. Conner, counsel for Hytera US Inc., met virtually with Ronald Repasi, Acting Chief Engineer, Office of Engineering and Technology (“OET”), as well as Ira Keltz, Dana Shaffer, Paul Murray, Michael Ha, Howard Griboff, and Jamie Coleman, from OET; Jeffery Goldtharp, from the Public Safety and Homeland Security Bureau (“PSHSB”); and Justin Faulb of the Wireline Competition Bureau (“WCB”) (collectively, “Staff”).

During the conversation, we discussed the circumstances surrounding the addition of HCC’s name (with respect to specific equipment) to Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (P.L. 115-232; 132 Stat. 1918) (“2019 NDAA”). HCC noted that the prohibitions of the NDAA were limited to telecommunication and video surveillance and included a Capability Exception and a Use Qualification. We observed that, under the Capability Exception, equipment that cannot route or redirect user traffic or permit visibility into any user data packets that it might transmit, is excepted from Section 889; and that, under the Use Qualification the NDAA only applied to the extent that the equipment was used for public safety/national security. We discussed how the Capability Exception and Use Qualification applied to HCC’s land mobile radios (LMR/DMR) equipment; in particular, that HCC’s LMR/DMR equipment was not interconnected with the public switched network and should be viewed as categorically excluded. We also discussed the 2018 CFIUS investigation of

DUANE MORRIS LLP

505 9TH STREET, N.W., SUITE 1000 WASHINGTON, D.C. 20004-2166

PHONE: +1 202 776 7800 FAX: +1 202 776 7801

DM3\7979133.1

Ms. Marlene S. Dortch
August 17, 2021
Page 2

HCC, and the fact that CFIUS had authorized the sale of PowerTrunk TETRA equipment without restriction.

We further discussed the Secure and Trusted Networks Acts of 2019 (Secure Networks Act) and its adoption of language from the NDAA to create the Covered List. HCC noted that the FCC's publication of the Covered List has caused some confusion in the marketplace. We addressed the FCC's position in the 2nd Report and Order in Docket 18-89 that the advanced communications systems covered by the Secure Networks Act related to broadband technology having greater than 200 kbps and noted how this excluded LMR/DMR technology. We further noted that the Secure Network Act also included a refined Capability Exception and Use Qualification similar to the 2019 NDAA; and that, as with the NDAA, HCC's LMR/DMR equipment is categorically not "covered equipment" under the Secure Networks Act.

The staff inquired regarding Hytera's non-LMR/DMR equipment, and specifically the use of HCC equipment with WIFI and cellular networks, and the use of video and camera equipment. HCC will file comments in this proceeding to address the staff's questions, including architecture diagrams showing Hytera's equipment used with third party WIFI and third party cellular systems.

Finally, we requested that the Commission revise the Covered List to clarify the Secure Networks Act's application to only broadband equipment and to include the Capability Exception. Specifically, we noted that the Exception appears to be indicated by a footnote notation, but the Commission's website fails to include the text of the footnote for the Capability Exception as set forth in the Secure Networks Act.

A Power Point presentation from the visit and two letters referenced during our discussion are attached.

A copy of this ex parte presentation is being submitted for the Dockets referenced above.

Respectfully submitted,

/s/ William K. Keane
William K. Keane
Patrick D. McPherson

Counsel for Hytera Communications Corporation Limited

Ms. Marlene S. Dortch
August 17, 2021
Page 3

cc: Ronald Repasi
Ira Keltz
Dana Shaffer
Paul Murray
Michael Ha
Howard Griboff
Jamie Coleman
Jeffery Goldtharp
Justin Faulb
Majorie K. Conner



Hytera Communications Corporation
PowerTrunk, Inc.
William K. Keane
Patrick D. McPherson
Hytera US
Marjorie K. Conner
August 13, 2021

Hytera Communications Corporation (HCC)

- HCC is a Chinese company, publicly traded on the Shenzhen stock exchange.
- HCC is not a state-owned enterprise (“SOE”).
- HCC’s founder and majority shareholder is not associated with and has never been a member of the Chinese Communist Party (“CCP”).
- The US subsidiaries of HCC are PowerTrunk and Hytera US.

CFIUS Investigation of HCC Ownership

- In early 2018, HCC submitted to a voluntary investigation by CFIUS regarding HCC's acquisition of Sepura plc, a UK-registered company, the parent of PowerTrunk, Inc.
- In July 2018, CFIUS issued a Letter of Assurance ("LOA") to HCC and PowerTrunk in order to "mitigate any national security risk" regarding the acquisition of PowerTrunk by HCC.
- The LOA identifies the TETRA radio equipment as authorized for sale in the U.S. by PowerTrunk and appoints the Department of Homeland Security (DHS) as the agency to monitor compliance with the LOA.
- In August of 2018, HCC's name was added to the 2019 NDAA without prior notice to HCC.
- PowerTrunk continues to sell its TETRA product in the US pursuant to the LOA including to major transportation systems in NJ and NY and to the Department of Defense (U.S. Army).

HCC'S Land Mobile Radio (LMR/DMR) Equipment

- Hytera US markets HCC's LMR/DMR equipment in the US
- Hytera US' equipment is sold to Private Land Mobile Radio Service ("PMRS") licensees, licensed under Part 90 of the FCC's rules.
- Hytera US does not sell its equipment directly to customers.
- Rather, Hytera US sells equipment to/through a network of dealers throughout the US.
- Hytera US dealers work with their customers to develop radio system design tailored to each customer's needs.
- Hytera US LMR/DMR equipment is designed to operate on Part 90 licensed frequency channels. It is not designed to interconnect with the public switched telephone network ("PSTN") or any Internet or broadband network.
- On customer request, dealers may design a radio system that interconnects Hytera radios to the PSTN or the Internet, but Hytera does not provide the interconnection equipment -- that must be obtained from another vendor.

Hytera single site DMR Repeater System



Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (P.L. 115-232; 132 Stat. 1918) (“2019 NDAA”)

- Section 889(a) generally prohibits government acquisition of covered telecommunications equipment *except* that it does not cover telecommunications equipment that cannot route or redirect user traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles. (Capability Exception)
- The Capability Exception means that, regardless of what is listed as “covered equipment,” the prohibition set forth in Section 889(a) cannot reach equipment that is not capable of interconnection. Without interconnection, the equipment cannot route, redirect or permit visibility into user data or packets.

The 2019 NDAA Included a Use Qualification

Section 889(f) of the 2019 NDAA defines covered telecommunications equipment or services to include, *inter alia*, **[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes**, video surveillance and telecommunications equipment produced by Hytera Communications Corporation.

The Communications Act Definition of Telecommunications Equipment

- Section 153(52) of the Communications Act of 1934, as amended, 47 U.S.C. § 153(52): The term “telecommunications equipment” means equipment, other than *customer premises equipment*, used by a *carrier* to provide telecommunications services, and includes software integral to such equipment (including upgrades). Emphasis added.
- For context: The term “telecommunications service” means the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used. 47 U.S.C. § 153(53)
- The term “telecommunications” means the transmission, between or among points specified by the user, of information of the user’s choosing, without change in the form or content of the information as sent and received. 47 U.S.C. § 153(50)

The 2019 NDAA Does Not Cover HCC's LMR/DMR Equipment

- Hytera does not manufacture or market video surveillance equipment or telecommunications equipment subject to the 2019 NDAA due to the Capability Exception.
- Should there be HCC equipment that does not fit within the Capability Exception, that equipment could still fail to meet the Use Qualification and so not qualify as Covered Equipment.

Secure and Trusted Networks Act of 2019 (P.L. 116-124) (“Secure Networks Act”)

- The Secure Networks Act appears to introduce confusion about exactly what equipment is “covered” by referring to it as “communications equipment” rather than “telecommunications equipment.”
- Any confusion is dispelled by the further refinement of the Capability Exception limiting listed equipment to only such equipment
 - capable of routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles (Section 2(b)(2)(A)); or
 - capable of causing the network of a provider of advanced communications service to be disrupted remotely (Section 2(b)(2)(B); or
 - otherwise threaten national security or the security and safety of U.S. persons.

The Secure Networks Act is Directed to Broadband Equipment

- “Communications equipment or service” means “any equipment or service that is essential to the provision of advanced communications service” (Section 9(4)).
- Section 706(c) of the Telecommunications Act of 1996 defined Advanced Telecommunications Services capability without regard to any transmission media or technology, as “high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology.” 2nd Report and Order, para. 55.

The Second Report & Order in Docket No. WC 18-89 Confirms that the Secure Networks Act is Directed to Broadband Equipment

- FCC defines “communications equipment or service” as meaning “all equipment or services used in fixed and mobile broadband networks, provided they include or use electronic components.” 2nd Report and Order, para. 53.
- FCC interprets “advanced communications service” to include “services with any connection of at least 200 kbps in any direction.” 2nd Report and Order, para. 55
- This underpins the Commission’s concern for the PSTN and Internet/Broadband networks in WC Docket 18-89, and specific attention to Advanced Telecommunications Services with connection speeds of at least 200 kbps in either direction.

HCC LMR/DMR Equipment is Categorically NOT Included

- None of the definitions includes HCC-manufactured LMR/DMR equipment
 - It is not broadband equipment – it is not capable of interconnection
 - It cannot route or redirect user traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles

The Covered List on fcc.gov is not Fully Consistent with the Legislation

- The purpose of the Covered List is to “serve as a reference for interested persons to indicate the communication equipment and services that certain providers must remove from their networks, as well as the equipment and services to which the section 3(a) prohibition applies, the communication equipment and services eligible for reimbursement pursuant to section 4, and the equipment and services that form the basis for the reporting requirements in section 5.” 2nd Report and Order, para. 57.
- With respect to Hytera, the Covered List published at <https://www.fcc.gov/supplychain/coveredlist> does not include the Capability Exception set forth in both the 2019 NDAA and the Secure Networks Act (the “Legislation”). It does not accurately reflect the definitions set forth in the Legislation, and thus does not serve as a proper reference for the marketplace.

Publish a Revision to the Covered List

- Hytera asks the Commission to draw a bright-line distinction that clearly excludes from the Covered List land mobile radio equipment that fits the Capability Exception.
- The Covered List includes definitions found elsewhere in statutes and FCC interpretive rulings and the marketplace would benefit if these definitions were included on the Covered List, in full, so as to provide the fullness of Congress' intent.
- Correcting the information on the Commission's website would make the Commission's work more consistent with the Legislation.
- The clarifications requested to the Covered List are not specific to Hytera but instead would apply to any manufacturer identified and help reduce marketplace confusion.



BAKER'S COMMUNICATIONS, INC

POST OFFICE BOX 3179
LAKE CITY, FLORIDA 32056-3179

386-752-6494 TEL
800-437-2346 WATTS

August 9, 2021

To whom it may concern;

Baker's Communications Inc. is a 47 year old two way radio communication company, employing 15 people (all of which are US citizens with families). We have been a Hytera US Dealer since 2008 just after they started operations in Miami Florida.

We found that the Hytera LMR radios, not only has outstanding performance but outstanding quality. We found that the radios with their 3 year warranty, sells well in our market which comprises of Public Safety and large industrial companies.

Since the NDAA/FCC Covered List was put out thru the Public Notice (DA 21-309), we have been told that they (people from agencies and/or companies) are not to consider them for radio systems because they had been told that Hytera was a security risk.

However, the Notice advises that risk is with "video surveillance and telecommunication equipment" which I have never heard, read or seen any Hytera web sites showing, advertising the sale of or offering of video surveillance equipment. As far as telecommunication equipment, the only items Hytera sells is LMR which by its nature is a closed system which the owner or user controls.

We have quoted some interconnected items but these rely on third party items such as Cisco routers and switches.

We have just experienced another example of last minute cancelation from a bid (an Electric plant), after they were told that Hytera was a risk, even though one of their other facilities uses a Hytera system.

Competitors seem to be using the FCC Public Notice as a whisper campaign against our DMR offered product Hytera.

I can only attest to what I have experienced. In my 47 years in the two way profession, land mobile is and will remain a closed systems with any connection to the outside world having to be done by a third party, as I stated above.

As a very loyal and proud American, I have not seen anything to warrant Hytera US land mobile to be on the security risk list of equipment.

Thank you,

Douglas Baker

Douglas Baker
President



August 9, 2021

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554

Re:

Dear Ms. Dortch:

We are a dealer of two-way radio products based out of St Louis, Missouri. Our company has been in business since 1962. We are directly involved in the sales, installation, and service of the products we represent. Our company and subsidiaries employ 40 people. Every one of those 40 people are US citizens. We are a dealer for multiple lines of products including Hytera.

I am concerned that the federal government and the FCC are unreasonably targeting Hytera products as a security risk to users. This leaves potential purchasers with the impression that these products are used by the Chinese government to spy on users. This could not be farther from the truth. The Hytera two-way radio equipment is usually installed as a closed system. The system works very well without any connection to the public telephone network or the internet. In the rear case where we (and our customer) choose to carry the audio over the internet, we are required to use third party, non-Hytera equipment to accomplish this task.

We have sold, serviced, and installed Hytera two-way radio products we see no evidence that their equipment is able to be used as a spy tool for a foreign government. The analog and DMR equipment are designed as a closed system with any need to connect to the public telephone network or the internet to operate. 90% of our Hytera DMR sales fall into this category. In the case where we decide to use internet connectivity to transport audio traffic between repeaters, we use third party devises, not supplied by Hytera, to switch and route the traffic.

In our markets, there are competitors using the documentation of the FCC proposed rulemaking to scare end users. We have direct experience with numerous customers who have stopped purchasing Hytera products because of these unsubstantiated government accusations and proposed rulemaking.

Our experience with Hytera has shown them to be a big supporter of us as a US owned and operated small business. Most radio suppliers in our industry have an arm where they will sell



their products directly to end use organizations. Hytera is the one major exception. Hytera US sales always involve an American owned dealership. They provide us with sales leads and in the couple of cases where a large end user has attempted to purchase directly, Hytera has refused. They would rather loose a sale rather than cut out the locally owned dealer.

I realize there are companies whose products are being used in the USA to achieve the goals of a foreign government and I think they should be investigated and delt with. I also think that the federal government should not punish a company or it's American owned dealers because of imagery allegations.

Respectfully submitted,

A handwritten signature in black ink that reads "Steve J Guller".

Steve Guller, President
Warner Communications Corporation
1340 Baur Blvd
St. Louis, Mo 63132
(314) 993-7070